U. S. Department of Energy

Calendar Year 2000

Annual Report of the Chief Information Officer

Prepared January 2001

Department of Energy
Chief Information Officer 2000 Annual Report
Executive Summary

The Department of Energy (DOE) Office of the Chief Information Officer (OCIO) is committed to providing strong collaborative leadership and supporting senior management across the Department to enhance mission accomplishment via efficient and effective use of information technology (IT). Accomplishments described in the 2000 Annual Report demonstrate the following.

- A rapid response to increasing cyber security threats.
- Significant improvements to IT infrastructure.
- Advances in information architecture and standards.
- Maturation of the DOE IT Capital Planning and Investment process.

Other significant OCIO initiatives focused on electronic government, software quality assurance, spectrum management, knowledge management, and records management. These accomplishments demonstrate OCIO commitment to being the customers' provider of choice for IT advice, support, and guidance.

The year began with the successful transition to the new millennium. OCIO led the Department's Year 2000 (Y2K) efforts, working closely with the energy sector, the White House Information Coordination Center, and other Federal Agencies. Thirteen DOE offices participated in leap year rollover activities. Aggressive efforts to ensure Y2K compliance of mission-critical, nonmission-critical, and health and safety systems resulted in only 35 minor Y2K-related failures out of a universe of more than 200,000 systems. No major impacts were reported and all failures were corrected within two weeks of the transition.

Cyber security was significantly improved in 2000. Recent General Accounting Office (GAO) and DOE Office of Independent Oversight and Performance Assurance (OA) reviews have highlighted positive changes. New policies and guidance provide a consistent governance framework throughout the Department. OCIO received and analyzed nearly 90 DOE site Cyber Security Program Plans, and all sites are on track to demonstrate effective Security Program implementation. OCIO administered cyber security training and awareness for system administrators and managers and provided funding and oversight for initiatives to support a comprehensive Cyber Security Planning and Implementation process. Improvements to cyber security at DOE Headquarters and the DOE Corporate Network (DOEnet) included development of a site Security Assessment Program and Implementation Plan, as well as development of a site Cyber Security Program Plan. Headquarters' cyber security posture was strengthened by treating the many loosely connected networks as a single site.

OCIO completed the deployment of the DOEnet which achieved full operational status on October 1, 2000. This network connects 38 major Departmental operations and regional sites, utilizes state-of-the-art Asynchronous Transfer Mode (ATM) technology and cyber security

capabilities and is designed to transport business essential traffic supporting Departmental corporate systems.

The Common IT Infrastructure Services (CITIS) Pilot Program was initiated to demonstrate creation of a consistent, cost-effective technical infrastructure with efficient, centrally-managed operations and services. Utilizing the CITIS concept in 2000, an infrastructure support center was established, components for service monitoring and performance management were implemented, and a consistent office and operating environment framework was developed.

OCIO commissioned a Total Cost of Ownership (TCO) study to analyze costs of the DOE Headquarters distributed computing environment. The TCO study resulted in a benchmark that provides a baseline for improving costs and quality of OCIO support services.

In response to the Secretary's management reform initiative, OCIO evaluated the feasibility of including additional IT services in the DOE Working Capital Fund (WCF) and developed a phased approach to adding services. OCIO partnered with Lead Program Secretarial Offices and other Program Offices to develop service level agreements, costs, pricing algorithms, and exit policies. In mid-July 2000, 12 business plans covering 14 IT services were approved for inclusion within the WCF with the approval of the Executive Committee for Information Management (ECIM). Full implementation of this initiative is pending Congressional approval.

OCIO completed a Corporate Systems Information Architecture (CSIA), which provides a plan for modernizing corporate information systems and a mechanism for ensuring IT investments maximize corporate data sharing and interoperability while avoiding costly, duplicative systems. CSIA was developed with collaboration from representatives across the Department. CSIA creates the plan for migrating to the "to be" environment pursuant to the Clinger-Cohen Act of 1996 and Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*.

Electronic government (e-gov) activities focused on developing consumer-centric capabilities, improving web-based information and services, ensuring active participation in Presidential e-gov initiatives, and improving coordination within the Department's web community. Specific projects included redesigning the Department's home page to conform with the President's directive on electronic government and the restructuring management process; ensuring the top ten percent of DOE web pages complied with Section 508 of the Rehabilitation Act of 1973; and supporting the Federal CIO Council Firstgov initiative.

Tasked by the Deputy Secretary, OCIO led the development and implementation of a response to the Defense Nuclear Safety Board's *Technical Report 25 – Quality Assurance for Safety-Related Software at Department of Energy Defense Nuclear Facilities*, issued in January 2000. OCIO collaborated with the Software Assurance Subcommittee of the Nuclear Weapons Complex to develop three Departmentwide guidance documents and assisted the Departmentwide Systems Engineering Process Group in completing the first volume of the Departmental Information Systems Engineering publications series that documents a total systems approach to software engineering. OCIO developed a Notice on Software Quality Assurance (SQA), which mandates the establishment of SQA Programs by Departmental Elements.

OCIO Frequency Spectrum Management Program provided representatives to advisory and planning committees and participated in negotiations to gain certification for the High-performance Electromagnetic Roadway Mapping and Evaluation system and the Multispectral Thermal Imager Satellite system, as well as treaty changes with Mexico and Canada. A spectrum migration database was developed to manage the shift to narrowband technology. OCIO developed the Wireless Technology Program Strategic Plan and established the Wireless Information Technology Policies task to provide Departmental guidance and advice on wireless issues.

Two successful Knowledge Management (KM) pilots were conducted in 2000: a collaborative software pilot during the Year 2000 rollover monitoring activities; and a desktop portal and electronic mail records management system pilot at the Yucca Mountain site. OCIO participated in InterAgency KM groups and activities.

OCIO sponsored an extensive records management pilot to test records management software implementation with electronic mail. The pilot included selected Headquarters Program Offices with approximately 2,500 people. OCIO updated the Records Management Directive to clarify roles and responsibilities. The Records Management Program assumed responsibility for the Paperwork Reduction Act Program, including annual submission of the Information Collection Budget. OCIO submitted a Government Paperwork Elimination Act (GPEA) Implementation Plan to OMB. The annual Records Management Conference was sponsored by OCIO.

In March 2000, the Department received an Inspector General report citing the lack of desktop software standardization as a cause of high costs and inefficiencies. The OCIO IT Standards Program stepped up to this issue and initiated the DOE Desktop Software Guidance Working Group, which produced a consensus-based profile of desktop software standards, as well as a process for sustaining and expanding the desktop standardization effort. Other standardization activities included publication and distribution of the *Information Architecture Profile of Adopted Standards 2000*, which updates the 1997 version.

Efforts to mature the DOE IT Capital Planning and Investment process included developing IT management and use policies; establishing Program CIOs and plans for a CIO Executive Council; improving IT Governance processes via CIO quarterly Program reviews and meetings of the ECIM; expanding the Strategic Information Management process to include crosscutting Program functional areas; and identifying improved management control points in the Corporate Management Information Program.

Accomplishments and initiatives described in this report highlight the strategies employed and the progress made by OCIO in 2000 to continue improving Departmental IT management capabilities.

Department of Energy
Chief Information Officer 2000 Annual Report

Information technology (IT) has evolved into an essential component of the methods used to accomplish Department of Energy (DOE) missions. As such, IT is a key tool for attaining strategic goals, enhancing efficiency, and reducing costs. Working with Departmental organizations, the Office of the Chief Information Officer (OCIO) has an important role in ensuring the effective use of information technology to help organizations achieve mission goals. Crosscutting organizations, such as the Offices of the Chief Financial Officer (CFO), Field Integration Council (FIC), and Policy support the Chief Information Officer (CIO) in implementing corporate IT initiatives while balancing technology, security, and the Department's missions. During the past year, development of policies and guidelines provided efficiency and consistency in security and investment.

The following initiatives described in this report highlight the progress made and strategies used by the CIO to continue improving DOE IT management capabilities: Cyber Security, Infrastructure Activities, Departmental Information Architecture (IA) Project Completion, E-Government, Software Quality Activities, Wireless Program, Knowledge Management Activities (pilot), Records Information Management, Standards Activities, Final Year 2000 (Y2K) Roll Over Activities and Ultimate Success, Planning Activities, EC-Web Fielded at HQ, Strategic Information Management (SIM) Activities, and an Expanded set of Corporate Management Information Program (CMIP) Quarterly Reviews.

1. Cyber Security

In 2000, the focus of the Cyber Security Program has been to maintain the current Program and be sufficiently proactive to meet tomorrow's challenges. Currently, the near-term plan is to better integrate security implementation with line management responsibility, continue implementation of site cyber architectures (boundary protection, host and application-based controls), and improve risk management processes.

During 2000, DOE began developing a formal, comprehensive Departmentwide Cyber Security Management Program that integrates risk management processes and physical, technical, and administrative controls for ensuring confidentiality, integrity, and availability of DOE information assets. Under this Program, a framework of objectives, guiding principles, and security activities and functions, applicable to classified and unclassified environments, will be established to govern consistent implementation of cyber security management throughout the Department. These actions will continue during 2001.

Success in cyber security will only come from a continued and focused effort to deal with the increasing complexity of the threats and the rapid evolution of technology. This challenge can be met by ensuring the Department is sufficiently equipped and personnel adequately trained.

The CIO Cyber Security Program is divided into four functional areas: policy, planning, and performance measurement; training, education, and awareness; operations; and technical

capability and research and development. Specific accomplishments in each of these functional areas follow.

Policy, Planning, and Performance Measurement

The CIO developed the following policies and guidance to provide a consistent governance framework throughout the DOE complex.

- Cyber Security Architecture.
- Intent and Objectives of DOE Password Policy.
- Web Security Best Practices (Endorsement of effort by Carnegie Mellon University).
- Cyber Security Auditing and Monitoring Clarification.
- Departmental Endorsement of Cyber Risk Assessment Guidance and Statement of Generic Threats to Information Systems (Endorsement of effort by Carnegie Mellon University Software Engineering Institute's "Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework").
- Guidance Regarding Cyber Security Incident Reporting.
- Cyber Security Physically Incompatible Removable Media Clarification.
- Clarification of Policies on Downloading Information on Cyber Systems.
- Guidance Regarding the Sanitization of Unclassified Equipment.

In addition, the Department has:

- Received and analyzed nearly 90 DOE site Cyber Security Program Plans. These plans, required by DOE Notice 205.1 Unclassified Cyber Security Program, describe each site's Cyber Security Program and are to be updated at least every two years.
- Instituted a set of cyber security management indicators and a Cyber Security Performance Measures Program to evaluate progress at each DOE site.
- Hosted several meetings of Policy and Technical Working Groups. These groups were established to assist in the formulation of DOE Cyber Security Program policy and guidance and provide technical consultation to the CIO. The Policy Working Group has met four times and the Technical Working Group has met three times during calendar year 2000.

Training, Education, and Awareness

During the past year, the CIO has administered cyber security training and awareness for system administrators and managers, including the following courses.

- UNIX Security.
- Windows NT Security.
- Host Securities (web and mail servers) Network Security.
- Cyber Security Awareness for Managers.

In addition, the CIO is developing a coordinated Cyber Security Training, Education, and Awareness (TEA) Program to improve job performance of the DOE workforce as related to safeguarding information with which they work. To date, an effort to develop a comprehensive training program for the DOE workforce has been initiated. Training objectives developed by a crosscutting working group at the 2000 Department of Energy Computer Security Group Training Conference were expanded to encompass all aspects of a complete TEA Program.

Operations

The CIO has implemented operational enhancements that link to policies and training initiatives as part of a comprehensive Planning and Implementation process. The OCIO provided funding and oversight for these enhancements detailed below.

- The Computer Incident Advisory Capability (CIAC), located at Lawrence Livermore National Laboratory, functions as the DOE central reporting capability to track and analyze reported cyber security incidents, and identify trends, patterns, and other events of concern.

- The Independent Validation and Verification (IV&V) Program at Los Alamos National Laboratory functions to reduce the number and severity of unauthorized access to sensitive and classified information in DOE classified computer systems, as well as increase the robustness of information security systems throughout DOE.

- The Headquarters DOE Information Systems Security Management Program functions to ensure security vulnerabilities within Headquarters' information systems are identified and minimized.

- DOE site cyber security protection has been enhanced through the expanded use of firewalls and intrusion detection software, stronger passwords, improved system configuration controls, and reconfiguration of system and network connectivity to reduce vulnerabilities. The DOE Cyber Security Knowledge Center was created as a management tool for cyber security policy development, review, coordination, and document tracking.

Technical Capability and Research and Development

The CIO is identifying and developing necessary upgrades in electronic security that can be incorporated into the DOE architecture baseline to meet evolving threats and provide new capabilities to protect against future cyber-related incidents. Funding was established in fiscal year (FY) 2001 to support the establishment of a limited testing capability for commercial-off-the-shelf (COTS) cyber security products. During the remainder of FY 2001, the following technology capability enhancements are planned.

- Evaluating COTS cyber security products, integrating and testing products, tracking new technology, and assessing the impact and evolution of DOE technological security posture.

- The Technical Working Group will define a prioritized functional scope for tools to include in the cyber security toolkit and evaluate specific products that meet toolkit requirements.

2. Infrastructure Activities

Headquarters Cyber Security Initiatives

Several initiatives were undertaken to enhance security of the DOE Headquarters site and DOE Corporate Network (DOEnet). Headquarters networks were strengthened by treating Headquarters as a single sitewide network rather than as several individual, loosely-connected networks. DOEnet, which achieved full operational status on October 1, 2000, uses state-of-the-art technology, including cyber security, that supports all Departmental corporate business systems and other Departmental communication needs. Initiatives included the following.

- Development of the Headquarters site Cyber Security Program Plan (CSPP) to include cyber security operational policies and procedures in accordance with DOE Notice 205.1.

- Implementation of scanning and vulnerability assessments across the Headquarters site.

- Installation of enhanced intrusion detection and firewall capability on the Headquarters site network and on DOEnet connections to other sites.

- Protection of publicly-accessible web sites from external and internal threats by moving them to a secured, screened subnet protected by the Headquarters firewall.

The following specific actions were implemented or begun in 2000.

- The Deputy Secretary appointed the CIO as the central authority for Headquarters cyber security.

- The CIO established the Headquarters site Cyber Security Working Group (CSWG), which is chaired by the Deputy Associate CIO for Operations. The group collaborates on Headquarters cyber security policies, shares information regarding cyber security, and

discusses cyber security initiatives that impact Headquarters. All Headquarters organizations are represented.

- A Headquarters CSPP was developed that treats the entire Headquarters network as a site. The CSPP includes comprehensive Headquarters site cyber security policies, such as policies on network connection, use of modems, network monitoring, virus protection, incident response, and foreign national access. A Cyber Security Self-Assessment Checklist was developed to supplement technical and physical portions of the risk assessment and was incorporated into the Headquarters CSPP.

- A secure screened subnet was created that resides behind the firewall and utilizes a variety of hardware and software protective techniques. Over 45 publicly accessible DOE web sites were migrated to this subnet to protect them from external and internal threats.

- The Headquarters primary firewall was converted to a managed firewall service monitored 24 hours a day, 7 days a week, 365 days a year. All Headquarters services were migrated to the new firewall. Additional intrusion detection mechanisms were installed.

- The OCIO acquired and began to install additional firewalls and intrusion detection capability on the Headquarters infrastructure and the DOEnet.

- The OCIO acquired additional tools to detect, monitor, and react to cyber incidents.

- A Headquarters site Security Assessment Program and Implementation Plan was developed. This Program satisfies the requirement for Departmental self-assessment per DOE Notice 205.1. Two major levels of assessment are conducted: perimeter and Headquarters organizational.

    1. The perimeter assessment focuses on (1) Internet-based penetration testing of perimeter entry points, e.g., firewalls; (2) configuration security review of specific devices attached to the network, e.g., routers and switches; (3) review of documented policies and procedures. The initial assessment has been completed.

    2. The Headquarters organizational assessment focuses on the more than 20 organizations that comprise the Headquarters site. Assessment is ongoing and each organization will be assessed every 2 years. The assessment is similar to the perimeter assessment described above.

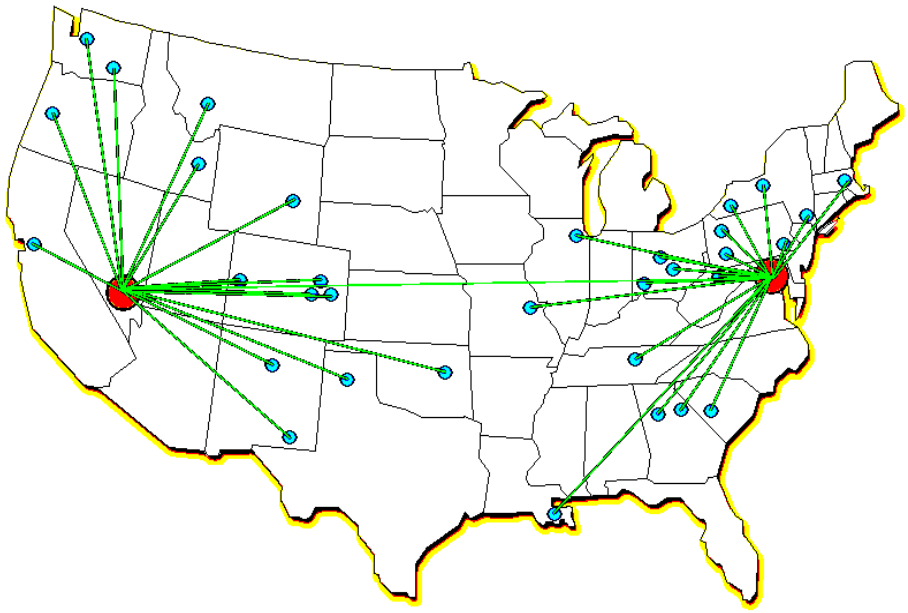
- Corrective actions were taken on the 600 switches on the Headquarters network to correct vulnerabilities as identified by the Office of Independent Oversight and Performance Assurance. Additionally, OCIO independently identified similar issues with other network devices and applied similar corrective actions.

- A Headquarters Configuration Management process was implemented. This process ensures that network components are meeting security standards by assessing the impact of changes before action is taken to implement.

DOE Corporate Network (DOEnet)

DOEnet achieved full operation status on October 1, 2000 with annual operations and maintenance costs funded through the Headquarters Working Capital Fund. This project began in 1998, when the CIO initiated a migration from the existing DOE Business Network (DOEBN), sponsored by the Office of Environmental Management (EM), to an improved network using state-of-the-art technology that supports all Departmental corporate business systems and other Departmental communication needs. Implementation of the network began in late 1999 and continued into mid 2000. The network currently connects 37 sites using Asynchronous Transfer Mode (ATM) technology and one site using the legacy frame-relay connection. The one remaining frame-relay site is scheduled to be converted to ATM in the second quarter of FY 2001.

DOE Corporate Network (DOEnet) Site Geography



All sites connected to the network agreed to connection requirements that significantly reduced the number of external Internet service providers (ISPs) and ensured that remaining ISP connections are appropriately firewalled, protecting the site and the network. Upgrades to each site have provided corporate network connectivity at a minimum of 1.544 Mbps ATM service and replaced field site data-only routers with routers capable of supporting simultaneous voice, video, and data services. Centralized network management has been fully implemented and provides higher reliability, improved trouble-shooting capabilities, greater operational efficiencies, increased accountability, and is essential to maintaining security.

Plans have been completed to develop and implement a cyber security strategy consistent with the Department's security architecture policies to ensure the privacy and protection of the DOE Corporate Network. Implementation of this plan will be done in phases, with the first 10 sites completed by December 2000.

Telecommunications Service Priority is in place and provides the network with priority restoration status in the event of a circuit outage. In addition, design improvements were made so the network remains operational if a hub site or hub circuit fails. In the event of a hub circuit failure, traffic is automatically rerouted with little to no loss of connectivity for the other DOEnet sites.

Common IT Infrastructure Services (CITIS)

The Common IT Infrastructure Services (CITIS) Pilot Program was initiated to demonstrate delivery of reliable, cost effective, and interoperable common IT system and services. It is challenged to provide seamless, consistent operating across Headquarters and, potentially, the Department. It was established to ensure future investments in information technology improve the Department's mission effectiveness through the delivery of common IT under a centralized services management strategy. It also aims to enhance electronic coordination and collaboration.

The following core and common services are to be delivered under the CITIS Pilot Program.

- Virtual Help Desk/User Support Services.
- Enterprise IT Infrastructure Systems Monitoring and Performance Management Services.
- Corporate Messaging and Coordination/Collaboration Services.
- Office Automation Standardization through a consistent operating environment.
- IT Service Level and Performance Management.
- IT Infrastructure Security.
- Dynamic Host Control Protocol (DHCP) automated IP address management.

The Pilot Program started on March 1, 2000 and is being executed in three phases.

1. Phase I analyzed the current core and common IT system services, identified the modernization requirements, and established respective modernization initiatives.

2. Phase II, currently in progress, is reviewing system options for modernizing the existing or new services, acquiring appropriate IT infrastructure components, installing and configuring systems or components, and deploying improved services within a pilot group for user evaluation and service expectation opinions. Pilot organizations include the Office of the Secretary, Management and Administration, Security and Emergency Operations, and the Office of the Chief Financial Officer.

3. Once the Phase II pilot is completed and evaluated as having met CITIS expectations, Phase III will commence. In this phase, CITIS services will be expanded beyond the pilot group to remaining organizations wanting to utilize CITIS services. This helps DOE move toward the objective of an IT infrastructure environment that centrally provides core and common IT

services across the Department at a reasonable price with enhanced service support, and electronically-measured performance of IT components. The current IT infrastructure is the starting point for future modernization and enhancement plans and a scalable IT infrastructure that can accommodate changing technology requirements.

Significant FY 2000 CITIS Program accomplishments included the following.

- Established a Headquarters Infrastructure Support Center for enhanced user support services to the desktop through employment of virtual remote control service restoration and interactive IT infrastructure components systems monitoring and performance management.

- Installed and established an enterprise IT infrastructure components monitoring and performance management system for ensuring maximum availability of common IT system services.

- Developed an Office Automation Standardization architectural framework for establishing a consistent office and operating environment within Headquarters.

- Designed performance reports for continual electronic measuring of the performance of the existing IT infrastructure and the supporting service contractors.

- Provision of modernized Headquarters Internet service to allow greater access and communications with external stakeholders, partners, and customers. Modernized Headquarters IT infrastructure security platforms to the public Internet for greater security of DOE information, resources, and data.

- Developed a future technology infrastructure architecture model and identified the corresponding technology transformation initiatives that need to be achieved for gaining future economy of scales in operation, and controlled and reduced IT costs through new and future enabling technology that allows centralized services management.

- Established a more economical means of providing remote access service for DOE telecommuters, mobile users, and Headquarters flexiplace workers to work from any location while ensuring security is not compromised and DOE information, resources, and data is protected.

Total Cost of Ownership Study of Headquarters Distributed Computing Environment

Total Cost of Ownership (TCO) study was completed to establish a benchmark of the Headquarters distributed computing environment. It includes costs for the acquisition, installation, management, and lifecycle support of client, server, and network assets. The TCO is intended to be a comprehensive model to help Program managers understand the cost of producing, owning, and using information technology components over time.

The Department conducted a competitive procurement for a consulting firm to perform the TCO analysis. Harris Technical Services Corporation, a General Services Administration contractor, was selected and an award was made in February 2000. The following tasks were accomplished.

- Performed a consolidated distributed computing environment benchmark analysis including qualitative and quantitative review.
- Developed a future state concept of operations that supports the required improvements.
- Recommended improvements for the distributed computing environment support within DOE Headquarters.
- Provided a business case for achieving the recommended improvements.

The approach used for conducting the study was two pronged, through interviews with representatives from Headquarters Program Offices and a web-based survey of DOE Headquarters end-users. The study was initiated in March 2000 and completed in August 2000. Twenty-one organizations participated in the interview portion of the study; 755 end-users from the Headquarters population of 6,573 responded to the web-based survey.

The survey covered six major areas.

- Information Architecture.
- Information Assurance (Security).
- Acquisition Lifecycle.
- Support.
- IT Management.
- User Perspectives.

The summary qualitative study results indicated all six areas had deficiencies and overall were marginally responsive to requirements. Significant improvements were required for each area.

The following table presents the TCO cost findings for the 21 participating organizations. It is divided into two sections, Direct (hard) costs and Indirect (soft) costs. Direct costs include hardware/software, operations, and administration. Indirect costs include end-user operations and downtime. These include activities such as solving their own computer problems, getting help from coworkers, casual learning, etc.

	DOE Actual (in millions)	Percent of TCO	Industry Average
Direct Costs (hard)			
Hardware and Software	**$13.8**	**12%**	**28%**
Operations	**$26.3**	**23%**	**18%**
Systems Administration	**$9.2**	**8%**	**6%**
Total Direct Costs	$49.3	44%	52%
Indirect Costs (soft)			
End-user Operations	**$61.8**	**55%**	**41%**
Downtime	**$1.0**	**1%**	**7%**
Total Indirect Costs	$62.8	56%	48%
Total Cost of Ownership	$112.1	100%	100%

Results of the TCO study were briefed on August 29, 2000, to the Executive Committee for Information Management (ECIM), which is co-chaired by the Deputy Secretary and the CIO. The ECIM requested the OCIO provide breakdowns of TCO costs by organization in addition to the consolidated summary.

Additional details providing direct cost results for selected DOE Program Offices using data collected for the enterprise TCO study were completed in October 2000. These were briefed individually to participating Program Offices. There were significant variations in individual Office's cost of services. Reasons for these variations are being examined on an office-by-office basis by the CIO and Program Office staffs.

The net result of the TCO study is a benchmark that provides a baseline for improvement for cost and quality of service provided in support of the DOE Headquarters distributed computing environment by the OCIO and Program Offices.

Working Capital Expansion for IT Services

As part of the Secretary's management reform initiative, the CIO was tasked to evaluate the feasibility of bringing additional IT Services into the DOE Working Capital Fund (WCF). The intent was to improve delivery of services to DOE organizations through consistent budgeting, billing, and auditing and procedures being applied to them. The ECIM approved the CIO phased implementation approach in March 2000 and requested the CIO accelerate the schedule for expansion of services into the WCF.

From April to mid July 2000, the CIO convened an IT Services Working Group. Representatives from Lead Program Secretarial Offices (LPSOs), as well as other Programs were requested to participate on the Working Group. All Program Offices had the opportunity to participate as the CIO wanted to fully vet and develop with Program customers the service level agreements, costs, pricing algorithms, exit policies, and other areas of interest to Program customers. The ECIM and the WCF Board were updated on the progress of this effort.

In mid-July 2000, the IT Services Working Group reached consensus on 12 business plans covering 14 IT services with a total estimated revenue in fiscal year 2001 of $22.6 million to be brought into the WCF. In late July 2000, these plans were presented to the ECIM for approval and subsequently to the WCF Board for approval and assistance for completing the expansion of these IT services into the WCF. The ECIM and subsequently the WCF Board approved the plan to expand the WCF with these IT services. Full implementation of this initiative is pending Congressional approval.

3. Departmental Information Architecture Project Completion

On June 15, 2000, the Executive Committee for Information Management approved the DOE Corporate Systems Information Architecture (CSIA). This decision was formalized by an August 8, 2000, memorandum from the Deputy Secretary to Heads of all Departmental Elements

that established the CSIA as the framework for making information technology investment decisions.

The approved CSIA establishes the mechanism and context for ensuring new systems and applications align most closely with established information technology infrastructure development and modernization goals to minimize replication of the functionality and data of corporate systems, and maximizes the use and sharing of established corporate data. The CSIA was developed in response to the Clinger-Cohen Act of 1996 and implemented guidance from the Office of Management and Budget.

The CSIA is a blueprint or roadmap that systematically and comprehensively defines the current "as is" state of operations; the target or "to be" operating environment for the corporate systems; and the plans for transition to the target. Representatives from Program and Staff Offices defined the flow of information needed to support common and crosscutting business functions and began identification of the underlying capability necessary to manage, maintain, and share information capability.

A complete and prioritized CSIA significantly benefits the Department by reducing the risk of building and buying systems that are duplicative, incompatible, and costly to maintain. It also enhances mission performance and capabilities by leveraging IT investments to directly facilitate mission activities. The architecture provides a sound managerial and technical basis for Strategic Information Management (SIM) studies and projects. In addition, the CSIA improves the timeliness and efficiency of information shared across the Department and with stakeholders by enhancing interoperability of systems and data; minimizing the stoppage or interruption of operations and mission activities by establishing a Departmentwide cyber security framework; and enhancing the protection of secure and sensitive information while minimizing the impact to the sharing of information.

4. E-Government

The OCIO undertook several activities to develop consumer-centric capabilities, improve web-based information/services, ensure active participation in Presidential e-gov initiatives and improve coordination within the Department's web community. These included redesigning the Department's home page, now Engergy.gov, and restructuring of management processes; ensuring compliance to Section 508 of the rehabilitation Act of 1973 on the top ten percent of DOE web pages; and supporting the Federal CIO Council's Firstgov initiative providing public access to Government information through a central web portal.

Redesign of the Department's Home Page and Restructuring of Management Processes

To compliment Presidential and Secretarial e-gov initiatives, the OCIO partnered with the Office of Consumer Information and the Office of Public Affairs to lead the redesign of the Department's portal home page. In a participatory process that involved all Program Offices, the redesign dramatically shifted the service model from focusing on serving specialist audiences to one that acknowledged and incorporated the needs of the general public. Content presentation

was transitioned from a structure that greatly mimicked the Department's organizational structure to one that emphasized perceivable subject/topic pathways and name brand identity, hence the use of the new name, energy.gov.

This effort also emphasized sustaining the timeliness, value, and access to information and services by broadening ownership responsibilities for energy.gov management and maintenance. This was accomplished through the creation of the Departmental Web Council whose membership includes representation from all Program elements. As an enabling tool, the Council charter includes language that focuses on perpetuating consumer-centric processes to ensure continued progress as well as coordinated improvements between energy.gov and home pages throughout the DOE complex.

In an effort to improve the quality, performance, and integrity of the DOE web site, access log analysis software for tracking visitor traffic and technical performance was implemented. This software provides content managers with a roadmap of what visitors look for when coming to the DOE web site. It allows DOE to provide more information that is of value to customers and eliminates information that may be useless or of little interest. From a web manager's standpoint, this allows streamlining of the site and better maintenance, thus providing a positive web experience for DOE customers. Long-term benefits of this tool provide DOE necessary data to maintain information currency, system functionality and security, and improve overall performance of the web servers, thus continuing to maintain service to the customer.

The use of this redesign and management process has been recognized by peer groups and media sources in the Washington, D.C. area. The Association for Federal Information Resource Management and Government Executive magazine have recognized the unique nature of this effort; the latter of which having publicly named energy.gov as one of the ten "Best Feds on the Web" for the year.

CIO Home Page Redesign

To improve communications within the Department's IT community, the OCIO web site was redesigned to improve content architecture and presentation. These efforts were undertaken in support of the functional business needs and objectives of the IT community. Information, services, and products provided were identified to provide the best value, accuracy, and coordination. This effort also included issuance of specific guidance for publishing documents on the web site to ensure the communication and collaboration value of this site continues to support the performance of IT professionals and efforts throughout the DOE complex.

Implementation of Section 508 of the Rehabilitation Act of 1973

In 1998, Congress amended several sections of the Rehabilitation Act of 1973 with the direct intent of improving access to electronics and electronic information by those with disabilities. This amendment mandates access to electronic products and computer applications and information posted to the world wide web for Federal employees with disabilities. To achieve objectives of this amendment, significant changes are required in the way electronics, computers, and computer software/systems are developed, procured, and implemented.

Full enactment of this amended legislation is not expected until the third quarter of fiscal year 2001; however, the OCIO has already initiated efforts to ensure compliance of Departmental web sites. Work has begun on primary level web sites to ensure access by those with disabilities through simple modifications. These modifications include incorporation of text equivalents for graphic representations as well as keyboard functionality for those unable to use conventional pointing devices. Efforts to date have resulted in most primary web sites being at or near Section 508 compliance prior to the mandated implementation deadline.

Additionally, the OCIO provides coordination within the IT community and with related offices, such as Procurement and Human Resources, to ensure compliance with Section 508. It is anticipated that Section 508 will dramatically affect the processes for technology procurement, implementation, and use. OCIO support staff have been dedicated to this task and are working with existing management groups within the IT and other specialist communities to provide guidance, coordinate issues, and implement policies within the allotted time.

Firstgov Initiative

In a December 17, 1999, memorandum to Heads of all Departments and Agencies, the President directs "…shall promote access to Government information organized not by Agency, but by the type of service or information that people may be seeking; the data should be identified and organized in a way that makes it easier for the public to find the information it seeks…." thus creating a central web portal also known as Firstgov.gov. On September 22, 2000, the President announced Firstgov.gov availability to the public.

During the first phase of development, the OCIO contributed web addresses and content to ensure a presence within the pinnacle access site. To compliment Firstgov.gov, design of the energy.gov site incorporated the goals of the President's memorandum as well as the style, format, and presentation objectives of Firstgov.gov to ensure information was organized in a manner that satisfied public requirements as information consumers. Knowing that Firstgov.gov development would continue into 2001, a permanent coordinator was detailed by the OCIO to assist Firstgov developers in creating simplified subject/topic categories and pathways to Departmental resources. Given the complexity of Departmental activities, this level of expertise was needed to ensure clarity and public perception of the Department as a national resource. This level of participation will continue until completion of this effort.

5. Software Quality

The OCIO was tasked by the Deputy Secretary to take the lead in a response to *Technical Report 25 – Quality Assurance for Safety-Related Software at Department of Energy Defense Nuclear Facilities,* issued by the Defense Nuclear Facilities Safety Board (DNFSB) in January 2000. The Department developed an approach that addressed the issues in three focus areas (1) infrastructure (i.e., policy, standards, and organization), (2) training, and (3) safety analysis and instrumentation and control (I&C) codes. The approach included a survey of software quality assurance (SQA) practices at defense nuclear facilities and an independent assessment of other

Government and industry organizations. Deliverables included a Departmental Directive on SQA; Departmental level summary reports on improving communications among safety and software staffs and organizations; and safety and software standards and training. A special group, the Safety Analysis Software Group (SASG), was formed to prepare a summary report addressing the three focus areas for software analysis and I&C software. The SASG will also identify a consensus set of standards and training for safety analysis and I&C software.

In addition to the January 2000 Technical Report 25, and after a review of Government Accounting Office (GAO) and Inspector General (IG) reports, it was determined there was a need for a Departmental Directive on SQA. In response to this, the OCIO developed a Notice on Software Quality Assurance, which mandates establishment of SQA Program(s) by Departmental Elements. Other recommendations in the technical report are being addressed by a Software Evaluation Group formed with participation from the major Programs with nuclear sites. The Notice outlined the objectives, applicability, critical components of an SQA Program, and responsibilities. The Notice was approved by the Deputy Secretary and will be developed into a Departmental Order.

To support the Order, the Software Quality Assurance Subcommittee (SQAS) of the Nuclear Weapons Complex and the OCIO collaborated to develop three guidance documents for Departmentwide use in improving requirements management, configuration management, and risk management. These areas were considered the most critical for improving DOE software development and maintenance project management. The three guidance documents were distributed to information management points-of-contact throughout the Department.

The Departmentwide Systems Engineering Process Group (DSEPG), a collaborative forum of staffs across DOE chaired by the OCIO, focused on information systems project management, engineering practices, and quality assurance, completed Volume 1, Information Systems Engineering Lifecycle (ISEG), of the Departmental Information Systems Engineering (DISE) series. The ISEG was prepared in response to a request by the steering committee to document a total systems approach to software engineering that began with information architecture. The document not only provides a total systems approach but also includes the high-level processes mandated by Clinger-Cohen such as SIM, Capital Planning and Investment, and Strategic Planning processes. The DISE discusses the usage of these processes for corporate and non-corporate systems. It also highlights major initiatives within the Department concerning security, safety, and standards. The intent is to provide a high-level view and show how these corporate processes and initiatives can and should be brought together on software and systems engineering projects. References are made to DOE corporate web sites where detailed information can be obtained.

6. Wireless Program

Dependence on wireless technology for voice, data, and video communications within the Department will increase significantly over the next 10 years. Enabling technology will soon be available to allow wireless connectivity for voice communication, Internet and e-mail access, and video teleconferencing from remote locations within major metropolitan areas via a single,

portable device. In addition, significant research and development progress by academia and the wireless industry for software programmable radios, ultra wide-band, and bluetooth technology offer new opportunities to DOE for interoperability, improved communications, and reduced equipment and installation costs.

Frequency Spectrum Management Program

The Frequency Spectrum Management Program's activities over the past year have successfully advanced, protected, and promoted spectrum-related information technology consistent with DOE business needs. Program representatives serve as advocates for DOE and have successfully promoted new policies in the best interests of the nation and Department. Spectrum use continues to be an essential and growing element of the DOE telecommunications infrastructure, and the Program continues to forge ahead in new scientific frontiers by seeking and negotiating national certification for new radio frequency-based technologies.

After long-term negotiations by the DOE OCIO representatives to the InterDepartment Radio Advisory Committee and Spectrum Planning Subcommittee, the Research and Development (R&D) 100 Award-winning High-performance Electromagnetic Roadway Mapping and Evaluation system (HERMES), developed by Lawrence Livermore National Laboratory for the Federal Highway Administration (FHWA), has received experimental certification. HERMES is a trailer-mounted sensing system that employs an array of 64 ultrawideband Micropower impulse radars to inspect bridge deck interiors. A vehicle can pull it across a bridge at traffic speed, collecting data that is processed into three-dimensional images. According to the FHWA, HERMES Bridge Inspector can save the public inconvenience and up to $100 million per year, since there is no need for bridge closure. Even more important, it results in higher confidence and safety in public roadways, and with further development, holds promise for other concrete inspection applications, such as railroads, tunnels, and runways.

After months of deliberation by the OCIO DOE Spectrum Planning Subcommittee representative, operational certification was received for the joint Los Alamos and Sandia National Laboratories and Savannah River Technology Center Multispectral Thermal Imager (MTI) satellite system. MTI primarily supports the Department's mission of nuclear proliferation detection; however, spin-off knowledge is expected to advance the state-of-the-art in multispectral and thermal imaging, creating a better understanding of the utility of these technologies. MTI began its 3-year mission by providing pictures of the fire-ravaged Los Alamos, New Mexico, area. These images are of special interest to Los Alamos researchers as the excellent spatial resolution and specific spectral range is useful in analyzing the burn area, tracking regrowth of trees and ground cover, and flood-mitigation efforts underway in the wake of the Cerro Grande fire.

Other accomplishments of the OCIO Spectrum Management team during FY 2000 included the following.

- Expansion of Los Alamos National Laboratory from 5 to 15 channel pairs.

- Expansion of Oak Ridge trunked communications system from 10 to 40 channel pairs.

- Expansion of Nevada Test Site from 10 to 58 channel pairs.

- Replacement of Idaho National Engineering and Environmental Laboratory trunked radio system with a narrowband system.

The National Telecommunications and Information Administration requirement for Agencies to vacate certain frequency bands and shift to narrowband technology by 2008 has a major financial and operational impacts on the Department. In 2000, the OCIO developed a Spectrum Migration database to serve as a tool to effectively and efficiently manage migration and narrowbanding of authorized radio frequencies, while assisting affected Departmental sites in assuring that transition occurs in a smooth and timely fashion. The database is used for tracking and reporting cases where lack of funding may make site operations vulnerable to interference or loss of operating authority.

On the international front, the Program continued participation in U.S. negotiations of a unilateral treaty with Mexico for controlled sharing of the spectrum for emergency response along the 75-mile border zone and an interim sharing agreement with the Canadian Coordinating Agency to modify provisions of the previous intergovernmental bilateral agreement and provide new 50/50 shared spectrum usage along the border.

Wireless Information Technology Program

The Department's Wireless Working Group (WWG), sponsored by the OCIO, is a collaborative partnership of wireless IT professionals that was originally formed to share ideas and address issues primarily concerning land mobile radio. It has expanded to include all aspects of wireless technology. The annual meeting was held November 28-30, 2000. The meeting was used to roll out the Wireless Technology Program Strategic Plan and recruit members to participate on working groups that will be formed to develop the Department Wireless Technology Management Plan, wireless IT architecture and standards, and policy and guidance documents.

7. Knowledge Management Activities

Knowledge Management (KM) activities are being developed throughout the Department that cut across many disciplines: information technology and management, record management, human resources, and library science. The CIO is gathering and sharing information on initiatives within the LPSO, Laboratories, and throughout the Department. Other potential activities have been identified.

The OCIO has been involved in several significant KM activities in 2000. OCIO staff members are active in interAgency groups and activities, including the Federal CIO Council's Knowledge Management Working Group and the Special Interest Group (SIG) on Best and First Practices. A Knowledge Management overview, *Managing Knowledge @ Work: An Overview of Knowledge Management*, was produced by the SIG and DOE contributed to this effort. This document may be found at www.km.gov under the Special Interest Group KM Strategies and

Best Practices. The Office is also a member of the Federal Knowledge Management Learning and Consulting Network, sponsored by the Federal Human Resources Development Council through the National Partnership for Reinventing Government (NPR) initiative.

Two KM pilots successfully developed in 2000 were the collaborative software pilot and desktop portal and electronic mail records management system pilot. The collaborative software pilot was successfully implemented during the Year 2000 rollover and follow-on activities are planned. The Yucca Mountain site has developed a desktop portal and electronic mail records management systems pilot that is being sponsored for presentation to the CIO Council's KM Working Group SIG on Best and First Practices.

The OCIO has been active in championing KM activities throughout the Department and Federal community. An Intranet portal pilot is being developed for Headquarters knowledge sharing. This is in response to the Workplace Improvement Network recommendations. The Executive Information system developed by the CFO was highlighted in the CIO Update Newsletter. Other initiatives in the Offices of Environment, Safety and Health, the CFO and the Energy Information Administration are being developed for publication.

The OCIO is active in the Department of Defense and Intelligence Community's Multimedia and Collaboration Technical Working Group (MCTWG) and participated in the Executive Summit Conference on Collaboration sponsored by the Mitre Corporation.

8. Records and Information Management

The OCIO has advanced the Department's commitment to manage recorded information in an efficient and effective manner in support of mission accomplishment and accountability. Significant accomplishments by the Records Management Division during 2000 are highlighted below.

The OCIO revised and updated the Records Management Order by clarifying roles and responsibilities in order to maintain a cost-effective Departmentwide Records Management Program that complies with the National Archives and Records Administration Act of 1984, as amended. The Order underwent Departmental review and will be published by the end of the year. The associated Manual that provides best practices and guidelines for implementation is being revised and will be published next year.

An extensive electronic mail records management pilot was undertaken for several Headquarters Program Offices during the year. The pilot has been initiated by OCIO and will continue into next summer, encompassing approximately 2,500 people. The intent of the pilot is to test records management software and implementation with electronic mail. This provides for management of electronic mail according to approved records disposition schedules. If that is successful, the pilot will be expanded to encompass all electronic documents within those Program Offices. Appropriate policy and guidance are being developed as part of the pilot process.

The annual Records Management Conference was held to promote effective and efficient records management within the Department. A successful Conference was held in Kansas City in June of 2000, with planning underway for next year's Conference in San Antonio, Texas. The Conference provides records management training for all levels of expertise with a special emphasis placed on training for people new to the field. Time is also provided for Departmentwide workgroups to meet, as well as the Records Management Council. Information sharing from Headquarters and field perspectives and networking are two benefits of the Conference in addition to the training opportunities.

Responsibility for the Paperwork Reduction Act Program, including the annual submission of the Information Collection Budget, was undertaken. This Program consists of identifying information collections imposed on the public (including contractors), receiving approval from the Office of Management and Budget (OMB) to collect the information, initiating review of the collections by the owning organization every three years to determine future status (renewal/withdrawal), and annually reporting on the reduction in the burden imposed by these information collections.

Government Paperwork Elimination Act (GPEA)

The Government Paperwork Elimination Act (GPEA, Pub. L. 105-277) requires that by October of the year 2003, when practicable, Federal Agencies are to offer the option of using electronic forms, electronic filing, and electronic signatures to conduct official business with the public or other Government Agencies.

The Department, through the OCIO, submitted a GPEA Implementation Plan to OMB on schedule. The plan stressed efforts on those transactions previously reported to OMB in response to the PRA. The Department's primary information collecting arm continues to be the Energy Information Administration (EIA). DOE reported on successes accomplished by two elements: EIA, and the Office of Scientific and Technical Information; and the significant use of the web to make available, in a pull technology, information from many individual Program Offices.

One major unfunded initiative needs to be automated, the one-stop-shopping initiative championed by the Office of Consumer Affairs. The objective of the initiative is to consolidate and automate the distribution of various publications available from the Department.

9. Standards Activities

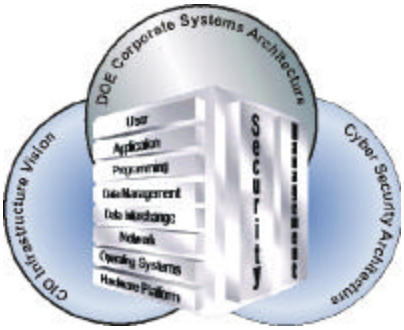
The DOE Information Technology Standards Program, a key component of the DOE IA, is the central mechanism for identifying, coordinating, adopting, implementing, and managing IT standards. The Profile of Adopted Standards and the DOE Technical Reference Model, required by the Clinger-Cohen Act of 1996 and OMB Circular A-130, *Management of Federal Information Resources*, helps link IT investments to the capital planning process.

.

Standards for the New Millennium

The *Information Architecture Profile of Adopted Standards 2000*, updating the 1997 version, was published and distributed DOEwide. The new profile contains 125 standards: 21 standards were added; 72 were revised, reaffirmed, or replaced by newer versions; 42 were removed; and 32 remain unchanged. The Department's move to desktop standardization was also facilitated during 2000 by the Standards Program. A DOEwide meeting was held to establish a Desktop Software Guidance Profile. The web version of the Profile is available at http://www-it.hr.doe.gov/Standards/DocsHtml/Profile2000_Menu.htm.

The new standards added to the Profile reflect the Department's evolutionary computing practices. The Department's cyber security initiative follows the Common Criteria standard, which provides a common, worldwide catalog of security functionality. Other new standards



reflect the trend toward a computing model based on a multi-tier, object-oriented, web-centric environment with COTS software replacing much traditional system development.

DOE Desktop Software Standards

On August 2-4, 2000, the IT Standards Program sponsored and convened a meeting open to all Departmental Elements to develop guidance to support desktop software standardization. The meeting achieved a consensus-based DOE Desktop Software Guidance Profile and a process for sustaining and expanding the desktop standardization effort.

Desktop software standardization has been a long-standing concern. The IT Council addressed the issue last year, but could not reach consensus. In March 2000, the Department came under fire from an Inspector General report citing the lack of desktop standardization as a cause of high costs and inefficiencies. The DOE IT Standards Program stepped up to this issue and initiated a Departmentwide effort to define desktop software standards.

More than 60 representatives from the Department's Lead Program Secretarial Offices, Operations Offices, National Laboratories, and field sites attended the initial meeting, formed the DOE Desktop Software Guidance Working Group (DSGWG), and established the DOE Desktop Software Guidance Profile. The Guidance Profile, which has been distributed Departmentwide by the CIO, focuses on desktop software products for administrative business computing and establishes guidance for the Department's target products in a 2001-2002 timeframe as well as de facto standards. The IT Standards Program is developing formal guidance.

DOE Desktop Software Guidance Profile

Status: / **Software:**	**Retirement**	**Containment**	**Current Products**	**Target by 2001-02**	***Suite***
Presentation	Lotus	Corel Presentations 6 Harvard Graphics PowerPoint 97	**PowerPoint 97*** PowerPoint 97/98 PowerPoint 2000 Corel Presentations 8	**PowerPoint 2000*** Corel Graphics 2000	**Office 2000***
Spreadsheet	Lotus Excel 4,3	Excel 5.0 Lotus 123	**Excel 97*** Excel 98 Lotus	**Excel 2000***	
Word Processing		WordPerfect 6.1	**Word 97*** Word 98 Word 2000 WordPerfect 8	**Word 2000*** WordPerfect 9	
Email	ccMail	Groupwise ccMail	Outlook 97/98 Notes Eudora Groupwise	Outlook 2000 Notes 9 Eudora x	
Browser	Internet Explorer 3.2	Internet Explorer 4 x	Netscape Internet Explorer 5.x	Netscape Internet Explorer 5.5	
Operating System	Macs & Win 3.1 DOS	Windows 95 NT 3.1 Win 98	Windows 98 NT 4 Win 95 Mac 8.6, 9	**Windows 2000*** Mac OS X Linux	

The DOE Desktop Software Guidance Profile identifies and targets desktop software products as guidance for Departmentwide planning, acquisition, and business information interchange. The products with an asterisk (*) indicate the Working Group's consensus on de facto Departmental desktop software standards.

Category Definitions	
Retirement	Obsolete or unsupportable software. The organization is actively expending funds to get rid of this software.
Containment	The organization is not purchasing or promoting the use of this software and is allowing it to be phased out.
Current Products	The current baseline of software the organization has in place and is supporting.
Target	Consensus direction the Department needs to take to establish desktop software standardization.

The DSGWG identified future areas for standardization, outlined a Sustainment process, drafted a charter, and defined a process to establish a desktop software acquisition approach. A number of these initiatives are ongoing with active participation. The IT Standards Program is the sponsor of the DSGWG and is planning follow-up activities in 2001.

10. Final Roll Year 2000 Over Activities and Ultimate Success

After the transition to Year 2000 (Y2K), DOE closely monitored safety, mission-critical, and nonmission-critical systems during the leap year rollover. Monitoring of internal systems commenced at 7:00 a.m. on February 28 and concluded at 9:00 p.m. on March 1. As expected, DOE sites remained Y2K compliant during these three days due to their extensive end-to-end system testing for the leap year roll over and the independent validation and verification that such systems should remain compliant during the roll over.

As it did during the millennium roll over, DOE worked closely with the energy sector and White House Information Coordination Center (ICC) during the leap year roll over. The Y2K status of DOE and private energy sector systems was reported to the ICC on a regular basis, and DOE staff were on-hand at the ICC to provide analysis, as needed.

Due to the success of the millennium roll over and the smaller degree of risk involved in the leap year roll over, the OCIO chose to decentralize Y2K data collection and reporting activities during the leap year roll over. To support rapid communications in the decentralized approach, the OCIO expanded use of the collaborative software used during the millennium roll over to facilitate data collection, aggregation, and reporting activities. The purpose of this pilot project was twofold - to fulfill DOE reporting responsibilities to the ICC, and evaluate benefits of expanding use of collaborative software within DOE.

Thirteen DOE offices participated in leap year rollover activities, including the Offices of the Deputy Secretary of Energy, Security and Emergency Operations, OCIO, Defense Programs, Science, Environmental Management, Policy, Public Affairs, Nonproliferation and National Security, International Affairs, Fossil Energy, General Counsel, and the Energy Information

Administration. Other Federal Agencies partnering with DOE included the Federal Energy Regulatory Commission, Nuclear Regulatory Commission, and Federal Emergency Management Agency. Finally, energy sector participants included the North American Electric Reliability Council, who monitored electricity sector status; the American Petroleum Institute, who monitored oil industry status; and the American Gas Association, who monitored gas industry status.

In response to DOE aggressive efforts to ensure mission-critical, nonmission-critical, and health and safety systems remained Y2K compliant, DOE sites experienced only 35 Y2K-related failures following the transition to the Year 2000 out of a total universe of more than 200,000 systems. No major impacts were reported as a result of these failures and all were corrected within two weeks of the transition.

11. Planning Activities

The DOE IT Capital Planning and Investment process was established in 1998 in response to the Clinger-Cohen Act of 1996, which directs Federal Agencies to use a comprehensive Capital Planning process for selecting, managing, and assessing IT investments. The Departmental corporate process provides an analytical framework for linking IT investment decisions to strategic objectives, mission achievement, and business plans. It applies to crosscutting corporate administrative and infrastructure initiatives. The OCIO supported the execution and maturation of the IT Investment process in alignment with the FY 2002 Budget process.

IT Investment Policy/DOECast

Efforts during 2000 to mature the IT Investment process included the following.

- Initial development of several IT management and use policies.
- Establishment of Program Chief Information Officers and plans for a CIO Executive Council.
- Improvement of IT Governance processes including meetings of the ECIM and CIO quarterly Program reviews.
- Expansion of the Strategic Information Management process to include crosscutting Program functional areas.
- Fine tuning of the Corporate Management Information Program to better plan, manage, and execute DOE IT corporate systems modernization efforts.

These policies, once implemented, work to ensure that a comparable level of rigor for IT investment processes is implemented Departmentwide.

IT Investment Governance

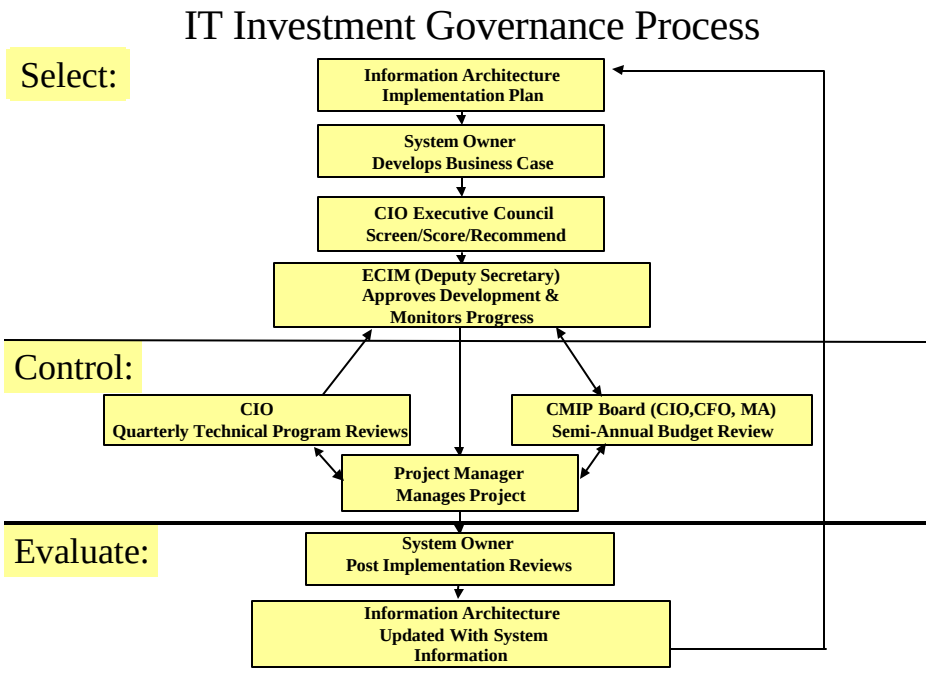
The Department began work and completed several actions to fine-tune the IT Governance process.

Program CIO Establishment

Since information technology is such an integral part of the Department's overall mission, the OCIO and the Office of the Deputy Secretary developed a course of action to ensure that IT management responsibilities, authorities, and accountabilities are appropriately assigned to a senior Program management official. In September, a memorandum entitled *Improving Management of Information Technology* was issued that directed each Lead Program Secretarial Officer to establish a full-time CIO position responsible for the coordination of IT responsibilities across the Program area, including IT Investment process oversight. All other Program and Staff Offices are required to designate a senior management official to be accountable for CIO responsibilities and authorities on a full or part-time basis as appropriate. The CIO is working with the organizations to develop implementation plans and position descriptions to meet requirements of the memorandum.

Governance Oversight Bodies

In the same memorandum, the Deputy Secretary directed the DOE CIO to establish and chair a Department CIO Executive Council. This Council, which replaces the Information Technology Council and the Information Management Steering Committee, reports to the ECIM, and may be delegated certain decision-making authorities currently exercised by the ECIM. The IT Governance Model that depicts the IT Investment process was revised to include the role of the new CIO Executive Council.



As part of the IT Capital Planning and Investment process, the CIO presents before the ECIM those IT projects that are of vital importance to the Department. The ECIM took the following actions, which were significant accomplishments for the IT Capital Planning and Investment process during 2000.

- Approved Business Management Information System - Financial Management business case.
- Approved Headquarters e-mail and web security architecture.
- Approved Business Case Development process for Corporate R&D Portfolio Management Environment (CME).
- Approved Corporate Systems Information Architecture.
- Approved expansion of information technology services within the Working Capital Fund.
- Approved recommendation from Nuclear Materials Strategic Initiative (NMSI) business case for development of an implementation schedule.
- Approved recommendation of the CME business case analysis to initiate project development.

Strategic Information Management Process

Another significant IT governance element is the Strategic Information Management (SIM) process, a General Accounting Office-sanctioned methodology used by the Department to link business needs and mission requirements with information technology when considering the modernization or development of corporate information systems.

The DOE SIM process relies on the knowledge and expertise from the DOE Federal and contractor communities who represent all areas of the business function being studied. By examining the issues and perspectives of all potentially impacted parties, costs and impacts of the decisions are fully understood before a project is implemented. This collaborative team develops a business case to assist DOE decision makers in determining the best strategy for implementing new or enhanced IT to support corporate (or Departmentwide) business needs. It also ensures strategic alignment among key functional elements, which helps realize significant cost savings and business improvement opportunities.

The 8-step approach to produce a SIM business case follows.

1. Establish the scope and boundaries for the project to ensure appropriate focus for the project.
2. Build the base case, which identifies the current environment and cost of doing business.

3. Examine best practices and industry trends to ensure direction taken is in agreement with best practice principles.

4. Identify high-level requirements of the business function being studied and the needs not currently being met.

5. Develop alternative approaches for meeting those needs.

6. Perform an analysis of benefits and costs on viable alternatives to show the full costs to implement and the return on investment projected over the lifecycle of the project.

7. Recommend the best solution and provide a preliminary action plan to initiate the recommendation.

8. Deliver the business case to the CIO and other stakeholders.

FY 2000 SIM accomplishments include development of business cases for the Department's NMSI and CME processes.

Corporate Management Information Program

The Department established the Corporate Management Information Program (CMIP) in FY 1998 as an investment initiative to replace outdated major DOE corporate systems. CMIP supports the reform of common and crosscutting business processes and the modernization of associated support systems. The Program strengthens linkages of corporate IT investments to business objectives to increase returns and reduce risk; consolidates systems that support the same business functions; improves data quality and integrity by eliminating redundancy of information across multiple systems; and refreshes obsolete systems and technologies to improve operating efficiencies and ensure Departmentwide interoperability.

Over time, CMIP has evolved and management oversight of initiatives has been established for two groups of modernization efforts. Corporate Business Systems, such as financial and human resource systems, are funded directly through CMIP and subject to investment decision-making by the CMIP Investment Review Board. In addition, other systems that are corporate in nature, but primarily support Program missions and functions, also come under the oversight of the CIO via CMIP review processes. The extension of CMIP oversight and processes beyond those initiatives funded by the CMIP Program ensures that all corporate systems are subject to similar requirements for business case development and investment review.

The Department has identified improved management control points for all CMIP initiatives, which include CMIP-funded and other Program-funded corporate systems. Improved management control points ensure that CMIP initiatives are adequately defined and managed in accordance with planned cost, schedule, and technical baselines; increase confidence that intended performance objectives will be achieved; ensure they are consistent and compatible with the Department's corporate systems information architecture; and improve the identification, mitigation, and management of project risk.

Through CMIP and SIM processes, the Department has defined several business process reform and system modernization initiatives that significantly improve business operations and control and reduce cost and risk. These initiatives are described below.

Corporate Business Systems

Business Management Information System - Financial Management (BMIS-FM)

BMIS-FM significantly improves response time for management and external customer financial data queries; reduces man hours required by elimination of multiple data entry processes; improves financial data integrity through reduction of data entry errors and elimination of multiple, inconsistent databases; enhances the Department's ability to achieve clean audit opinions on financial statements; and reduces costs through the elimination of redundant financial systems.

Corporate Human Resource Information System (CHRIS)

CHRIS reduces the amount of paperwork required for human resource processes; provides accurate, timely information to make sound human resource decisions; replaces redundant, outdated legacy systems such as the PERS portion of PAY/PERS (Payroll and Personnel system) and Departmental Training Information system (DTIS); and improves services and employee productivity through desktop human resources transaction processing.

Online Learning Center (OLC)

The OLC reduces the Department’s overall cost of training (including development, delivery, and associated travel); address GAO concerns over lack of training administration/management control; improve consistency of training across the Department; respond to Strategic Alignment Initiative 44 (develop a corporate approach for training) from the Secretary of Energy report of May 3, 1995, *Saving Dollars and Making Sense*; and improve the quality of learning opportunities for Departmental employees through reductions in learning time (30 to 40 percent less than classroom instruction), the provision of on-demand learning, better quality control and greater flexibility, and faster updates to training materials.

Department of Energy Network (DOEnet)

DOEnet improves the security posture for the Department by securing the corporate network behind an appropriate firewall; improves quality of network services by incorporating planned redundancy (extra hubs and connections) to ensure connectivity; reduces Departmentwide costs through a single supplier contract for telecommunications services; and improves the Department’s abilities to more effectively capitalize on technological advances (such as providing excess bandwidth to leave room for new services).

Procurement Modernization (EC-Web)

EC-Web supports e-Government Directives to improve and increase electronic service delivery by the Government; addresses Government Paperwork Elimination Act (GPEA; P.L. 105-277) requirements by creating a paperless procurement process for small purchases; and increases efficiency and effectiveness of the Department's procurement process by making a broad array of vendors from a single source available to small purchasers.

Foreign Travel Management System (FTMS)

FTMS improves the Department's security posture by providing accurate data on foreign travel by employees and contractors; reduces inefficient paper based processing of foreign travel requests; and improves the Department's ability to respond to Congressional and other queries about foreign travel by Department personnel.

Other Corporate Systems

Corporate R&D Portfolio Management Environment

In August 1999, the Under Secretary of Energy launched a SIM study to determine how best to modernize and streamline R&D management processes and move toward a corporate R&D portfolio management environment. The estimated Departmentwide costs for performing and supporting current R&D management processes total more than $200M, of which about 17 percent (more than $30M) represents process inefficiencies. The current process is disjointed, labor intensive, and complex. It requires multiple proposal and plan submissions, duplicative reporting of the same information in varying formats, repetitive data collection and entry, and manual data integration, all of which increase opportunities for error. In addition, the current R&D process is incapable of tracking a research project electronically from inception to completion or providing information on the composition of the Department's R&D portfolio.

The Corporate R&D Portfolio Management Environment provides the Department with a single, rational and comprehensive approach to manage and maintain an R&D portfolio. This corporate approach improves planning and management of research projects (lifecycle tracking of proposals/funding); enhances the ability of scientists to communicate and share results and lessons learned with colleagues Departmentwide; reduces administrative costs for R&D Programs and scientific organizations as the need for multiple proposal submissions are eliminated; reduces budget formulation cost through the integration of automated systems with existing site project management systems; supports better reporting to Congress, OMB, and the White House's Office of Science and Technology Policy; and allows the Department to respond to requirements set forth in the Federal Financial Assistance Management Improvement Act of 1999 (P.L. 106-107) to automate the Grants process. The cost of this CMIP initiative is approximately $17M, and it is expected to yield $39M in annualized productivity gains.

Corporate Nuclear Materials Information System

The NMSI SIM project was chartered to develop a coherent and integrated corporate strategy to improve the management of a vast array of national security, research, and excess nuclear materials and their supporting systems. There is an estimated $200M currently being spent annually by the Department to manage, use, track, and report information on the nation's nuclear materials inventory. Careful review of the underlying systems architecture that supports the management and maintenance of the nuclear materials inventory found that currently nuclear materials are managed in a non-integrated and uncoordinated manner, and inconsistent business practices are used in accountability and information management activities. Multiple, non-connected databases that must be manually reconciled to each other have resulted in inconsistent data and information being provided to other organizations, Agencies, and the public. This has put the Department at risk of being erroneously perceived as not maintaining effective controls over the nation's nuclear materials. In addition, many of the systems supporting nuclear materials management have not been upgraded to take advantage of the latest technologies and integration opportunities.

The recommended business case strategy has the potential to avoid as much as $66M annually in future years after it is fully implemented. The proposed activities, to be implemented over a 5-year time frame, reduce the potential for erroneous data, as well as reduce the various inefficiencies related to maintaining multiple disparate systems. The activities also establish common business practices and an integrated systems architecture to support the nuclear materials stewardship business functions.

Annual Information Technology Conference (AITC)

The Department of Energy established this annual conference on office information technology to address issues regarding the acquisition, implementation, operation, and maintenance of information technology and office automation environments in support of the missions, goals, and objectives of DOE and Programmatic Offices.

Primary objectives of the Conference are as follows.

- Promote interoperability, portability, and scalability of computerized applications across networks of heterogeneous hardware, software, and communications platforms.

- Provide a forum for Departmental and DOE contractor personnel to exchange strategic, tactical, and operational information about planned and operational information technologies and office automation support systems.

The theme of the January 2000 conference was *The Information Technology Evolution*. Keynote addresses focused on DOE corporate challenges in enterprise architecture, infrastructure, networks, cyber security, corporate systems, and DOE Laboratory information technology opportunities and challenges.

Ten interactive workshop sessions, linked to a keynote address, presented views from the perspectives of OCIO, LPSO, Operations Offices, National Laboratories, and various contractors. There were in-depth explorations of the complex issues and challenges facing the Department. Contrasting approaches were presented for examination and scrutiny, and interactive audience participation was solicited.

As an outcome of this conference, a CIO AITC Information Technology Strategic Plan – Working Draft was developed, which outlined six objectives. Each objective contains AITC Workshop and LPSO issues and approaches, as well as Information Technology Council discussions and approaches to resolving these issues.